A'N method for loading input data into a program when performing an authentication between electronic cash cards and a security module.--.

On page 1, delete line 2.

On page 1, before line 3, insert --Related Technology

A2 Various prior--.

On page 1, line 3, delete "of this kind" and delete "and".

On page 1, line 4, change "the devices are based, inter alia, on" to --with devices being based on, among other things,-- and change "EP" to --European Patent Application Number--.

On page 1, line 6, change "Methods of the kind referred to here are known" to --Related methods are described-- and change "from" to --in--.

On page 1, line 17, change "EP" to --European Patent Application Number--.

On page 1, line 19, change "locations" to --areas--.

On page 2, line 2, change "(P95114) proposed a method whereby" to --in a method described in PCT Patent Application Number 95114--.

A3

On page 2, line 4, change "machine and, during" to --machine. During--.

On page 2, line 7, change "balance; after that" to --balance. Subsequently,--.

On page 2, line 8, change "made; and finally" to --made. Finally--.

On page 2, line 11, change "module; following" to --module. Following--.

On page 2, before line 14, insert --Summary of the Invention--.

On page 2, line 14, change "The object" to --An object--.

On page 2, line 15, change "the 'electronic cash purses'" to --electronic cash cards.--

On page 2, before line 18, insert --The present invention therefore provides a method for loading input data into an algorithm when performing a cash transaction authentication between an electronic cash chip card and a security module.

A4 Brief Description of the Drawings

The present invention may be more easily understood with reference to the drawing, in which:

Fig. 1 shows a block diagram of a method in accordance with the present invention.

Detailed Description

Fig. 1 shows a block diagram of the method of the present invention for loading input data into a program when performing a cash transaction authentication between an electronic cash chip card and a security module, the chip card including a stored credit balance. As shown in block 102, a cash amount requested, preferably input by the cardholder, is debited from an electronic cash chip card using a security function. The requested cash amount is added and stored in a cash amount summing counter of a security module, as shown in block 104. Then, as shown in block 106, input data is subdivided into a plurality of data blocks. According to the present invention, the data blocks are loaded into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter, as shown in block 108. Next, at least one additional feedback is introduced into the linear-feedback shift register following the at least one downstream counter, as shown in block 110. Lastly, as shown in block 112, the at least one additional feedback is switched off after a predefined number of clock pulses.--

On page 2, delete lines 18-30.

On page 3, line 3, delete "as well,".

On page 3, line 6, delete "the".

On page 3, line 11, change "the condition being" to --where it is required--.

On page 3, line 18, change "can" to --may-- and change "in that" to --with--.

On page 3, line 19, change "are" to --being-- and change "functions' =" to --functions," that is,--.

On page 3, line 21, change "can" to --may--.

On page 3, line 23, between "then" and "be" insert --may--.

On page 3, line 24, change "strong enough" to --sufficiently powerful--.

On page 3, line 26, change "insofar as" to --in that--.

On page 4, line 1, change "The" to --An--.

On page 4, line 3, change "used:" to used. Exemplary steps and features include:--.

On page 4, line 5, change "0. Additional" to ---Additional--.

On page 4, line 8, change "1. Input" to ---Input--.

On page 4, line 13, change "2. A" to ---A--.